FAQ

CYBERSECURITY IS WTF

Hackers kicken op vakantieperiodes

*Het is vandaag **W**onderbaarlijk eenvoudig om een organisatie te hacken. En wel om de eenvoudige reden dat werknemers en management onvoldoende bewust zijn van de gevaren van het internet. In vakantieperiode zijn we zelfs nog minder dan gewoonlijk op onze hoede. Bijvoorbeeld omdat we inspringen voor collega's en hun werkomgeving minder beheersen. Of omdat we lekker lui op het strand minder alert zijn. Net daarom is het **T**otaal **F**undamenteel dat iedereen binnen de organisatie voldoende bewust is van de nooit aflatende bedreiging. Want samen staat u sterker tegenover kwaadwillige hackers.*

Auteur: Nick Huysmans, Supervisor BDO Risk Advisory Services

WAT IS SOCIAL ENGINEERING?

Social engineering is een vorm van psychologische manipulatie. Het is een vaak gebruikte techniek waarbij de hacker probeert een of meerdere computersystemen aan te vallen of de computerbeveiliging te kraken via de zwakste schakel binnen uw organisatie, met name de mens. Het doel van de aanval? Het verkrijgen van vertrouwelijke of geheime informatie. De hacker zal u op een heel geloofwaardige manier vragen naar een – op het eerste gezicht niet schadelijke – website te surfen en uw wachtwoord of gebruikersnaam in te vullen. Of hij doet zich voor als de CEO met de vraag om een bedrag te storten. Kortom, het is duidelijk dat social engineering zich niet beperkt tot één methode.

"Cybersecurity overstijgt de technologie. Het is een opleidingsprobleem. Uw mensen moeten deel uitmaken van uw oplossing."

WIE ZIJN DE HACKERS VAN VANDAAG?

Vergeet 'hackers in hoody's'. Er zijn vier grote groepen hackers: (1) misdaadbendes, (2) staat en overheid, (3) hacktivists en (4) uw eigen werknemers. Die laatste groep is waarschijnlijk de interessantste of alvast de meest verrassende. En toch, de eigen werknemers hebben immers toegang tot computersystemen en vertrouwelijke, geheime informatie. Wij merken bijvoorbeeld dat wanneer werknemers misnoegd zijn (bijv. bij een mislopen promotie of ontslag) ze de grenzen van het toelaatbare overschrijden. Veel situaties bieden hen de kans om de eigen organisatie aan te vallen. Vaak is het probleem dat werknemers, zonder dat management op de hoogte is, te veel toegangsrechten hebben tot computersystemen of applicaties.

PHISHING, OK! MAAR WAT IS SMISHING?

Een valse e-mail van de bank of de vraag om zo snel mogelijk uw wachtwoord te wijzigen? U kent ze vast wel, de typische phishingmails. Dit type valse e-mails blijft enorm populair bij hackers. Waarom? Omdat werknemers en management vaak onvoldoende bewust zijn van de gevaren die erachter schuilen. Bovendien zitten hackers niet stil. Ze vinden telkens nieuwe technieken uit, zoals 'smishing'. Dat staat voor sms-phishing. Hackers sturen vandaag de dag behalve valse e-mails, ook valse sms-berichten om u in de val te lokken. Maak daarom uw mensen voldoende bewust en houd ze up-to-date over de nieuwste trends in cyberlandschap.

PHISHING VS. SMISHING – VOORBEELDEN

'HR vraagt om een vakantieaanvraag goed te keuren' (phishing)

Check altijd de volgende basiselementen van de e-mail:

- Is het e-mailadres correct?
- Zijn er zichtbare spelfouten?
- Zet de e-mail u onder druk door bijvoorbeeld gebruik te maken van **'BELANGRIJK'**, **'ACTIE VEREIST'**?
- Vraagt de e-mail uw logingegevens of kredietkaartinformatie?
- Is de boodschap van de e-mail te mooi om waar te zijn?
- Zweef met de muis even over de 'klik hier'-button en controleer de website waarop u zou doorklikken.
- Wees extra aandachtig wanneer u e-mails ontvangt op uw mobiele toestel. Wie op vakantie is, leest zijn e-mails vaak minder oplettend.

'U ontvangt een sms van het hotel: Via deze website kunt u gratis een extra nacht boeken.' (smishing)

Dat kan wel eens een typisch geval van een 'smishing' zijn. De hacker probeert u in de val te lokken door u een aantrekkelijk en vaak 'te mooi om waar te zijn'-aanbod te doen. Ga niet blindelings in op zo'n sms, maar stem even af met het hotel of het bericht legitiem is.

GRATIS WIFI OP HET STRAND. IS DAT TE VERTROUWEN?

Op vakantie? En op zoek naar gratis wifi? Denk dan zeker twee keer na voordat u zich verbindt met één van de vele gratis wifipunten bij het strand of in het hotel. Vaak zetten hackers valse wifipunten op, in de hoop dat u gaat connecteren waarna ze via deze weg data kunnen stelen. Wanneer u binnen de EU reist, raden we aan 'mobile roaming/mobiele data' te gebruiken en niet de vaak malafide, gratis wifipunten. Wilt u toch gebruikmaken van gratis wifi? Vraag dan in het hotel welke connectie veilig is.

GRATIS WIFI? USB-DROPPING?

Welke schade kunt u oplopen door op een vals wifipunt in te loggen? Zodra u met het netwerk verbindt, kan de hacker alle verkeer tussen u en uw respondent(en) in het oog houden. Bijvoorbeeld wanneer u op een social mediawebsite uw wachtwoord ingeeft. Stuurt u een e-mail uit, besef dan dat de hacker die kan onderscheppen.

U parkeert de auto in het hotel en vindt daar een USB-stick met een gekend logo. Benieuwd naar de vakantiefoto's of de informatie die op de stick staan? Niet doen! USB-sticks worden vaak door hackers gebruikt als toegangspoort tot uw computersystemen. Bent u zeker dat er geen virus op de stick staat dat uw computer kan overnemen? Beheers uw nieuwsgierigheid en laat de stick liggen of gooi hem in de prullenmand.

CEO-FRAUDE, DAT KENT U WEL!

Het is een misvatting dat CEO-fraude te maken heeft met een frauderende CEO. Bij CEO-fraude in de context van cybersecurity doet een hacker zich voor als de CEO. En stuurt hij bijvoorbeeld een zorgvuldig opgebouwde e-mail uit naar een selectief publiek binnen de organisatie. Met daarin bijvoorbeeld de vraag om een bedrag te storten op een rekeningnummer omdat hij/zij het op dat moment niet zelf kan. Die techniek wordt vaak gebruikt tijdens de vakantieperiode. En dan meestal nog op het moment dat de CEO zelf met vakantie is. Dat maakt het valse bericht extra geloofwaardig.

SOCIAL MEDIA ZIJN VEILIG, TOCH?

Het gebruik van de social mediasite an sich is veilig, maar de info die gebruikers beschikbaar stellen niet altijd. U deelt leuke vakantiekiekjes of laat weten dat u drie weken op vakantie trekt? Wees op uw hoede wanneer u informatie post op social media. Hackers weten die informatie te vinden en kunnen ze tegen u gebruiken. Door middel van sociale media krijgen hackers inzicht in zowel uw professionele activiteiten als in uw privéleven.

"Vergeet 'hackers in hoody's'. De eigen werknemers vormen een van de vier grote hackersgroepen."

KUNT U WORDEN GEHACKT ALS U WORDT GEBELD?

Zeker. Die techniek heet 'voice solicitation' of 'vishing'. Een hacker doet zich voor als een te vertrouwen partij – uw bank bijvoorbeeld – en probeert u via een telefoongesprek privéinformatie te ontfutselen of laat u naar bepaalde websites surfen. Om het nog geloofwaardiger te maken, kan de hacker u zelfs bellen met het nummer van een voor u gekend persoon ('spoofing'). Laat u dus zeker niet misleiden wanneer u verdachte telefoons ontvangt van gekende derde partijen.

WAT KUNT U DOEN OM UZELF EN UW ORGANISATIE BETER TE BESCHERMEN?

Op vakantie? Waarom eens niet digitaal detoxen? Drie weken lang de computer en smartphone volledig aan de kant. Zalig toch?

Op kantoor? Weet dan dat cyberbewustzijn verbetering stimuleert. Oplossingen, zoals een 'security awareness'-training of een gecontroleerde en ethische phishingaanval, helpen uw organisatie bewust te worden van een degelijke cybersecurity. Beschouw het als een cursus (cyber)zelfverdediging voor uw medewerkers. Herhaal de cursus op regelmatige tijdstippen zodat uw medewerkers de juiste attitude eigen maken en leren de juiste reflexen te hanteren. Zo maakt u van uw organisatie een veiligere werkplek.

VRAGEN OVER DE DO'S-AND-DON'TS BIJ CYBERAANVALLEN OF HACKINGS?

Neem contact op met de specialisten van ons 'Cybersecurity'-team: steven.cauwenberghs@bdo.be, francis.oostvogels@bdo.be of nick.huysmans@bdo.be